IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of	Conf. No.: 8934
ROXBURGH, et al.	Atty. Ref.: LB-36-2015
Serial No. 10/594,124	TC/A.U.: 2165
Filed: September 25, 2006	Examiner: Bai D. Vu

For: METHOD AND APPARATUS FOR COMMUNICATING DATA BETWEEN COMPUTER DEVICES

* *

June 15, 2010

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the Examiner.

TABLE OF CONTENTS

(I) REAL PARTY IN INTEREST

The real party in interest is British Telecommunications public limited company, a corporation of the country of Great Britain.

(II) RELATED APPEALS AND INTERFERENCES

The appellant, the undersigned, and the assignee are not aware of any related appeals, interferences, or judicial proceedings (past or present), which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

(III) STATUS OF CLAIMS

Claims 2-6, 8 and 16-18 are pending and have been rejected. The rejections of claims 4-6, 8 and 16-18 are being appealed. No claims have been substantively allowed.

(IV) STATUS OF AMENDMENTS

No amendments have been filed since the date of the Final Rejection dated November 19, 2009.

(V) SUMMARY OF CLAIMED SUBJECT MATTER

A listing of the representative independent claims and each dependent claim argued separately is provided below including exemplary, but not limiting, reference(s) to reference numerals, Figure(s) and page and line number(s) of the specification.

The invention of the claims relates to a system 100 and a method for notifying a client application sub-system, e.g., 110, that is connected to a server sub-system, e.g., 250, via a gateway 200, that it should initiate a secure authenticated connection with the server sub-system 250 when an event related to a communication between the client application system 110 and a further user, e.g., 19, occurs (e.g., Figs. 1-3, p. 8, lines 7-18, p. 10, line 25 to p. 11, line 32).

Claim 16 relates to a system 100 comprising:

programmed computer devices (100, 200, 300, Fig. 1) which execute program code (Figs. 4-5) to provide a first sub-system 250 and a gateway 200 for offering services provided by the first sub-system 250 to one or more application hosting sub-systems (110, 120, 130) via the gateway 200 and a data communications network between said gateway 200 and sub-systems (110, 120, 130), p. 8, lines 7-18;

the gateway 200 and each application hosting sub-system (110, 120, 130) being arranged to permit each application hosting sub-system (110, 120, 130) to initiate a secure and authenticated connection 410, 415 from each application hosting sub-system (110, 120, 130) to the gateway 200 via a non-secure data network connection (Figs. 1-3, p. 8, lines 7-18, p. 8, lines 5-29) and

the gateway 200 being logically connected to the first sub-system 250 to enable the services provided by the first sub-system 250 to be provided to each application hosting sub-system (110, 120, 130) via a secured and authenticated connection (p. 3, lines 25-27, p. 8, lines 7-18),

the gateway including notification means 220 for initiating an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems (110, 120, 130) and transmitting over this or each such connection a notification 450 for notifying said one or more of the application hosting sub-systems (110, 120, 130) that it should initiate a secure authenticated connection 460 with the gateway 200 when the notification means 220 is requested so to do by any one of the services offered by the first sub-system 252 (Fig. 3, p.11, lines 5-32).

Claim 17 relates to a method of offering services provided by a first sub-system 250 to one or more application hosting sub-systems (110, 120, 130) via a gateway 200 which includes a notification means 220 for notifying one or more of the application hosting sub-systems (110, 120, 130) that it should initiate a secure authorized connection with the gateway 200, the gateway 200 and each application hosting sub-system (110, 120, 130) being arranged to permit each application hosting sub-system (110, 120, 130) to initiate a secure and authenticated connection from each application hosting sub-system (110, 120, 130) to the gateway 200 via a non-secure data network connection, and the gateway 200 being logically connected to the first sub-system 250 to enable the services provided by the first sub-system 250 to be provided to each application hosting

sub-system (110, 120, 130) via a secured and authenticated connection (Figs. 1-3), the method comprising:

sending a request from a service wishing to set up a secure and authenticated connection to an application hosting sub-system (110, 120, 130) that the notification means 220 send a notification 445 to a respective application hosting sub-system (110, 120, 130) to notify it that it should initiate a secure authenticated connection with the gateway 200 (steps 525, 530, 700 in Fig. 5, p. 11, lines 13-22, p. 14, lines 8-20);

initiating from the notification means 220 to the application hosting sub-system (110, 120, 130) an unauthenticated and unencrypted connection and transmitting over this connection the notification 450 for notifying said application hosting sub-system (110, 120, 130) that it should initiate a secure authenticated connection with the gateway 200 (Fig. 3, p. 11, lines 13-16, step 700 in Fig. 5, p. 14, lines 13-24);

causing the application hosting sub-system (110, 120, 130) to set up a secure and authenticated connection with the gateway 200 in response to receipt of the notification 450 (Fig. 3, p. 11, lines 18-32); and

communicating with the initiating service via said connection (see 460 in Fig. 3, p. 11, lines 24-32).

Dependent **Claim 5** relates to the system of claim 16, wherein

the notification means 220 includes means 640 for permitting each service provided by the first sub-system 250 to specify the number of times which a notification is to be retried in the event of failure to deliver the notification and means (671, 672) for server retrying to deliver the notification up to the specified number of times in the event

of failure to deliver the notification over the non-secure network (Fig. 6, p. 15, lines 14-17, p. 17, lines 1-8).

(VI) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(i) Whether claims 2-6 and 16-18 are unpatentable under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement.

(ii) Whether independent claims 16 and 17 are obvious under 35 U.S.C. §103(a) over Grantges, Jr. et al. (US 6,510,464) in view of Wilding (US 2005/0050329).

(iii) Whether dependent claim 5 is obvious under 35 U.S.C. §103(a) over Grantges, Jr. et al. (US 6,510,464) in view of Wilding (US 2005/0050329) and further in view of Osterman (US 5,935,211).

(VII) ARGUMENT

(i) Whether claims 2-6, 8 and 16-18 are unpatentable under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement.

The Examiner stated that the limitation "the gateway including notification means for initiating an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system" of claim 16, and the limitation "initiating from the notification means to the application hosting sub-system an unauthenticated and unencrypted connection and transmitting over this connection the notification for notifying said application hosting sub-system that it should initiate a secure authenticated connection with the gateway" of claim 17, do not have support in the instant specification, see p. 4 of the Office Action of November 19, 2009.

Section p. 11, lines 13-16 of the instant specification recites "As a result of the processing performed by notification server 220, the notification server 220 initiates a simple (unauthenticated and unencrypted) TCP/IP connection 450 with listener 112 and transmits over this connection a notification (the nature of which will be described in greater detail below) to listener 112". This section teaches that the notification means sets up an unauthenticated and unencrypted connection and then it transmits a notification message over this connection. As can be seen in Fig. 3 of the instant specification, the

notification server 220 sends a "Transmit Notification" message 450 to Listener 112. According to the above section, this message is sent over an unauthenticated and unencrypted connection, which is initiated by the gateway 200 that includes the notification server 220 (Fig. 2). The Listener 112 is part of the application hosting sub-system 110 (see Fig. 2).

Moreover, p. 11, lines 18-22, of the instant specification ("Upon receipt of the notification, listener 112 forwards this notification via forward notification communication 455 to a notification processing module (not shown) within the main (client application specific) part 11 of the application 110 which processes the notification and thereby establishes that it should attempt to contact the SMS service plug-in 257"), teach that the notification is sent as a result of being requested to do so by any of the services (e.g., the SMS service 257), since it is the SMS service that needs to be contacted by the application hosting sub-system (for example, for providing the user of iLocate application 110 (e.g., "Dad") with information about another user (e.g., "Dad"'s daughter "Kate"), see p. 8, lines 9-18.

In response to Appellant's arguments, the Examiner stated that "the claimed application hosting sub-system and the listener 112 in the supported portion are interpreted as not being connected or related. There is not any definition that describes the claimed application hosting sub-system is the listener 112", see Advisory Action of March 14, 2010.

As can be seen in Fig. 2 of the instant specification, the listener 112 is part of the client application hosting sub-system 110. Box 112 is within the confines of the

application hosting sub-system, and it is not shown by itself or within the gateway 200 or within the mobile operator 300. Moreover, the above mentioned section, p. 1, lines 18-22 of the specification, infers that the listener 112 is part of the application hosting sub-system, receives the notification, and transmits it to the notification processing module of the application hosting sub-system.

For the above reasons, independent claims 16 and 17 have support in the instant specification. Dependent claims 2-6, 8 and 18 also fully comply with 35 U.S.C. §112, first paragraph.

(ii) Whether independent claims 16 and 17 are obvious under 35 U.S.C. §103(a) over Grantges, Jr. et al. (US 6,510,464) in view of Wilding (US 2005/0050329).

The USPTO has the burden under 35 U.S.C. Section 103 of establishing a prima facie case of obviousness. *In re Piasecki*, 745, F.2d 1468, 1471-72, 223 USPQ 785, 787-88 (Fed. Cir. 1984). It can satisfy this burden only by showing that some objective teaching in the prior art, or that knowledge generally available to one of ordinary skill in the art, would have led that individual to combine the relevant teachings of the references to arrive at the claimed invention. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). Before the USPTO may combine the disclosures of the references in order to establish a prima facie case of obviousness, there must be some suggestion or rationale for doing so. *In re Jones*, 958 F.2d 347 (Fed. Cir. 1992). Prior art references can be combined to render an invention obvious only if there is some apparent reason, either in the references themselves or in the knowledge generally available to one skilled

in the art, to combine them. *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 82 USPQ2d 1385 (2007). Even assuming, *arguendo*, that a given combination of references is proper, the combination of references must in any event disclose the features of the claimed invention in order to render it obvious.

None of the prior art teaches or suggests "the *gateway* including notification means for *initiating* an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that *it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system*", emphasis added, as required by claim 16 (similarly for claim 17).

To generally appreciate differences between Appellants' claimed invention and known prior art systems, it is important to form a mental image of the main integers of Appellants' claims and how they relate to one another. In overview, such an image needs to be along the lines of either Fig. 1 or 2 of this application. A first sub-system 250 hosts a number of services 255, 256, 257, all of which can be contacted (in a basically normal client/server manner) through the horizontal services layer 252 (this is, in essence, the gateway). In parallel with the horizontal services layer 252, there is also a notification server 220 discussed below. Finally, some applications (hosted on one or more application hosting sub-systems) not only want to contact the services 255, 256, 257 from time-to-time (as per conventional systems), but also want to receive notifications from these services from time-to-time when appropriate.

Since a system requires fairly complex functionality to be able to set up a connection initiated by someone else in a safe and secure manner (note this is the functionality provided by the horizontal services layer 252 in Fig. 1), it is normal for the services 255, 256, 257 to not have any mechanism for directly contacting what are effectively their clients. Thus, normally, if a service has any notifications for sending to a client, it simply waits until that client next contacts the server and then lets it "know" that there is a notification waiting for it.

However, in the invention of claims 16, 17, there is added a notification server which can pass a simple (non-secured) message to any of the applications (i.e., the clients) and let them know to contact the notifying service. This does not require any complexity on the part of the applications (i.e., the clients) and is safe.

Thus, the claimed architecture enables a plurality of services (255, 256, 257) to offer their services in a secure manner, with the ability to notify their clients (110, 120, 130, 140, 150) when necessary – and all of this is done in an efficient manner whereby the services do not need to worry themselves about how to implement either the security requirements (252) or the notifications (220) since this is all handled centrally by the gateway layer (200 - especially 252 and 220) and the clients do not need any complex functionality to allow a connection to be set up by a third party in a secure manner.

Regarding claims 16 and 17, the Examiner acknowledged that Grantges does not disclose the features indicated above, and turned to Wilding for the missing limitations, see p. 6 of the Office Action of November 29, 2009.

Wilding discloses a method such that a customer system 102 can establish a secure connection with an organization system 104 using a public network, allowing the customer system 102 to communicate with the organization system 104 in a secure manner, while authenticating the identity of the customer system 102 to the organization system 104 and vice versa (Fig. 1). According to the method, once the customer has registered with the server, the customer system initiates a connection, [0028]. A temporary Server Public Key is sent from the service gateway to the customer system using the TCP connection initiated by the customer system. A series of encryption packages is sent back and forth between the gateway and the customer system over this TCP connection initiated by the customer system, until a remote, secure authenticated and encrypted connection has been established between the service client 108 and the service gateway 110.

The Examiner asserted that the process "starting from the step of transmitting the Temporary Server Public Key from the service gateway 110 to the service client 108 (i.e., interpreted as a notification to verify the authenticated information); until the step of establishing secure, authenticated and encrypted connection between the service gateway 110 and the service client 108" disclosed by Wilding reads on the above missing limitation, see p. 6 of the Office Action of November 29, 2009.

The Examiner's assertion is not true. In Wilding, it is clear from paragraph [0028] ("Once the customer has registered with the server, a remote service session can be established. Referring to FIGS. 3A-3B, a flow chart illustrating the steps for establishing a remote session is shown. In step 302, the customer system initiates a connection. The

service client 108 establishes a Transmission Control Protocol/Internet Protocol (TCP/IP) connection, or session, to the service gateway 110. This is similar to having the customer use the telnet protocol to connect to a remote system through the Internet, although the following steps ensure a much higher level of security than a telnet connection"), emphasis added, that the connection is initiated by the customer system. All the encryption packages being sent back and forth between the customer and the service gateway are sent over the TCP connection initiated by the customer system.

In contrast, claim 16 requires "the *gateway including notification means for initiating* an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems". In other words, in the invention of claim 16, it is the gateway that initiates an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems, for the purpose of asking the one or more application hosting sub-systems to initiate a secure connection with the gateway, not the one or more of the application hosting sub-systems that does the initiation.

Furthermore, regarding Grantges, the Examiner identified an "options page" being sent by gateway web server 34 in a message 78 to client computer 22 (Fig. 2), the "options page" presenting a list of authorized applications 24_1, 24_2...24_3 for selection by user 18 of client computer 22, as the claimed "when the notification means is requested so to do by any one of the services offered by the first sub-system", see p. 6 of the Office Action of November 29, 2009.

However, even assuming *arguendo* (which Appellant does not believe to be the case) that message 78 including an "options page" corresponds to "notification means",

this cannot be interpreted as it being requested by any one of the services offered by the first sub-system (identified as the applications 24_1, 24_2…24_3 by the Examiner), as required by claim 16. Instead, in Grantges, the notification is requested by the user 18 (which was identified by the Examiner as the claimed application hosting sub-system). Message 78 is not generated in response to a request from the any one of the Applications (App. 1, App. 2, App.3) of Grantges, but in response to a request issued from the DMZ proxy server 34 which itself was initiated as a result of receiving a request from the web browser 22 for connection to the system 20 as a whole. In addition, an options page presented to the client computer 22 merely represents what is available to the client computer, not a specific request by one of the services offered by the first sub-system to the client computer to initiate a secure authenticated connection with the gateway.

It is clear in Grantges, e.g., col. 8, lines 18-20 ("User 18, via client computer 22, through its web browser, initiates a request 64 for authentication…"), that the connection is initiated by the user. Connections between the web browser 22 of the client computer and the system 20 (including DMZ Proxy server 34 and the Application Gateway 38) are always initiated by the web browser. Thereafter, information is passed back and forth using the connection, but it is not initiated by the web server 44 (corresponding to the claimed gateway including notification means), as required by claim 16 ("the *gateway including notification means for initiating* an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems", emphasis added).

One of ordinary skill in the art would not have looked into modifying Grantges in order to include notification means. In Grantges, there is no perceived need for

notifications to be sent to the users 18. This is because the services provided by applications 1, 2 and 3 are conventional services adhering to a classic client/server model where servers simply respond to an input request from a client. The only mention of applications in Grantges (col. 5, lines 24-30) does not suggest that they might ever need to send a notification to a user to contact the server, nor accordingly is there any discussion of any mechanism for sending such notifications.

For the above reasons, claim 16 is allowable. Claim 17 includes limitations similar to those of claim 16 and is also allowable.

It is respectfully requested that the rejection of claims 2-6, 8 and 18, all dependent form claim 16 or 17, also be withdrawn.

(iii) Whether dependent claim 5 is obvious under 35 U.S.C. §103(a) over Grantges, Jr. et al. (US 6,510,464) in view of Wilding (US 2005/0050329) and further in view of Osterman (US 5,935,211).

Regarding claim 5, the Examiner cited Osterman for the limitation that the notification means specifies the number of times up to a specified number a notification to an application hosting sub-system is to be sent in case of failure to deliver the notification. Osterman discloses a system involving a server and a client (Fig. 1, col. 4, lines 11-23), wherein the server keeps a list of active processes in the client system, by entering time entries of various active processes in the client and based on the list, removing inactive processes (col. 7, lines 42-53).

However, Osterman fails to cure the deficiency of Grantges/Wilding, namely the lack of teaching of initiation of notification by the gateway. As discussed above, one of

ordinary skill in the art would not have looked into modifying Grantges in order to include notification means. In Grantges, there is no perceived need for notifications to be sent to the users 18. Moreover, Osterman merely teaches removing inactive processes of the client from the notification list, not specifying the number of times which a notification is to be retried in the event of failure to deliver the notification.

CONCLUSION

In conclusion it is believed that the application is in clear condition for allowance; therefore, early reversal of the Final Rejection and passage of the subject application to issue are earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Leonidas Boutsikaris/
Leonidas Boutsikaris
Reg. No. 61,377

LB:tlm
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

(VIII) CLAIMS APPENDIX

2. The system according to claim 16 in which the notification takes the form of a non-executable data file.

3. The system according to claim 2 in which the notification takes the form of a simple text file containing an extensible Markup Language, XML, document.

4. The system according to claim 16 wherein the notification means is operable to run separate threads for controlling the forwarding of separate notifications to the client application.

5. The system according to claim 16, wherein the notification means includes means for permitting each service provided by the first sub-system to specify the number of times which a notification is to be retried in the event of failure to deliver the notification and means for server retrying to deliver the notification up to the specified number of times in the event of failure to deliver the notification over the non-secure network.

6. The system according to claim 16 wherein a single notification server receives notifications from plural services and forwards these to plural client application hosting sub-systems.

8. The system according to claim 16,

wherein the first sub-system is a backend sub-system which provides services to the gateway, and

wherein the server sub-system acts as a trusted intermediary between each application hosting sub-system and the backend sub-system.

16. A system comprising:

programmed computer devices which execute program code to provide a first sub-system and a gateway for offering services provided by the first sub-system to one or more application hosting sub-systems via the gateway and a data communications network between said gateway and sub-systems;

the gateway and each application hosting sub-system being arranged to permit each application hosting sub-system to initiate a secure and authenticated connection from each application hosting sub-system to the gateway via a non-secure data network connection, and

the gateway being logically connected to the first sub-system to enable the services provided by the first sub-system to be provided to each application hosting sub-system via a secured and authenticated connection,

the gateway including notification means for initiating an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated

connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system.

17. A method of offering services provided by a first sub-system to one or more application hosting sub-systems via a gateway which includes a notification means for notifying one or more of the application hosting sub-systems that it should initiate a secure authorized connection with the gateway, the gateway and each application hosting sub-system being arranged to permit each application hosting sub-system to initiate a secure and authenticated connection from each application hosting sub-system to the gateway via a non-secure data network connection, and the gateway being logically connected to the first sub-system to enable the services provided by the first sub-system to be provided to each application hosting sub-system via a secured and authenticated connection, the method comprising :

sending a request from a service wishing to set up a secure and authenticated connection to an application hosting sub-system that the notification means send a notification to a respective application hosting sub-system to notify it that it should initiate a secure authenticated connection with the gateway;

initiating from the notification means to the application hosting sub-system an unauthenticated and unencrypted connection and transmitting over this connection the notification for notifying said application hosting sub-system that it should initiate a secure authenticated connection with the gateway;

causing the application hosting sub-system to set up a secure and authenticated connection with the gateway in response to receipt of the notification; and

communicating with the initiating service via said connection.

18. Computer readable storage media containing a program or suite of computer programs for controlling one or more computer processors to carry out the steps of claim 17 during execution of the computer program or suite of programs.

(IX) EVIDENCE APPENDIX

None.

(X) RELATED PROCEEDINGS APPENDIX

None.